

IN THE UNITED STATES DISTRICT COURT
FOR CHATTANOOGA

IN THE MATTER OF THE SEARCH OF
THE ENTIRE PROPERTY LOCATED AT
3657 SHIRL JO LN Apartment C,
East Ridge, TN 37412 including,
the person and cell phone of Paul
Douglas Nida.

Case No. **1:20-mj-161**

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Damarise Goehring, being duly sworn, depose and state as follows:

INTRODUCTION AND TASK FORCE OFFICER BACKGROUND

1. I have been an Officer with the Chattanooga Police Department since November 2013 and have been a Special Victims Investigator since April 2018. As of December 2019, I have been a Task Force Officer with the FBI, authorized to enforce federal law and request federal search warrants. As a Special Victims Investigator, I investigate adult and juvenile Rapes, Sexual Assaults, Animal Abuse, Domestic Assaults, and any other crime deemed necessary by the Chief of Police. As a Task Force Officer, I investigate Child Pornography cases and any other cases involving sexual abuse of children.
2. The statements contained in this affidavit are based upon my investigation, information provided by other law enforcement agencies and partners, and on my experience and training as a Task Force Officer of the FBI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I

have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a violation of Title 18, United States Code, Sections 2252(a)(2) and 2252A(a)(2), which make it a crime to receive or distribute child pornography in interstate commerce and Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B), which make it a crime to possess child pornography, will be found at the location identified below and on the person of Paul Douglas Nida.

3. This affidavit is being submitted in support of an application for a search warrant to search the premises at 3657 Shirl Jo Lane #C, (Apartment C) East Ridge, Tennessee 37412 (herein referred to as the Subject Premises) and the person of Paul Douglas Nida and his cell phone, which are each fully described in Attachment B of this affidavit. I have probable cause to believe contraband and evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252(a)(2) and 2252A(a)(2) and Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B), are located within SUBJECT PREMISES and on the person of Paul Douglas Nida. I submit this application and affidavit in support of a search warrant authorizing a search of the SUBJECT PREMISES, the person of Paul Douglas Nida, including his cellphone, as further described in Attachment B, incorporated herein by reference, and to seize evidence, fruits, and instrumentalities of the foregoing criminal violations, as more fully described in Attachment A, which is also incorporated herein by reference.

APPLICABLE LAW

4. Title 18, United States Code, Sections 2252(a)(2) and 2252A(a)(2), make it a federal crime for any person to knowingly receive or distribute child pornography that has traveled in interstate or foreign commerce.
5. Title 18, United States Code, Sections 2252(a)(4)(B) and 2252A(a)(5)(B), make it a federal crime for any person to knowingly possess any material that contains an image of child pornography that has been mailed, or shipped, or transported in interstate foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped, or transported in interstate or foreign commerce by any means, including by computer.

BACKGROUND INFORMATION

6. As is the case with most digital technology, communications by way of computer and smart phones can be saved or stored on the devices used for these purposes. In addition to electronic communications, a computer user's online activities generally leave traces in the web cache and history files of the browser used. A forensic examiner can often recover evidence which shows that a computer or smart device has accessed certain files and imagery and possibly when they were uploaded or downloaded. Such information may be maintained indefinitely until overwritten by other data.

7. I have had both training and experience in the investigation of computer-related crimes, including those involving child pornography. Based on my training and experience, I know the following:
- a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
 - b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable, or via wireless connections such as "Wi-Fi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.
 - c. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer, smartphone, or other internet-capable device.
 - d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - including computer hard drives, external hard drives, CDs, DVDs,

and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual’s person. Smartphones are also often carried on an individual’s person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files,

reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

CHARACTERISTICS OF CONSUMERS OF CHILD PORNOGRAPHY

8. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who produce, advertise, transport, distribute, receive, possess, and/or access with intent to view child pornography (i.e., "consumers" of child pornography):

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing

children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including in “hard copy” and electronic format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material in the privacy and security of their home or some other secure location. Many individuals who have a sexual interest in children or images of children and who have hard copies of child pornographic material retain that material for many years.

d. Likewise, such individuals often maintain their digital or electronic child pornography in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor’s residence, inside the possessor’s vehicle, or, at times, on their person, or in cloud-based online storage, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis, sometimes in an attempt to destroy evidence and

evade law enforcement. I know through my training and experience that this type of behavior is often seen in individuals who have some level of technical expertise, are aware of law enforcement efforts to investigate child pornography offenses, gain access to child pornography on anonymized dark web networks like Tor or encrypted mobile applications (which are sometimes perceived by offenders as being “safe” from law enforcement detection), or struggle with their addiction or attraction to child pornography.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals’ computers and other digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.

f. Such individuals also may correspond with and/or meet others to share information and materials, often retain correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain contact information for individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

h. I submit that even when individuals use a portable device (such as a mobile phone) to access the Internet and child pornography, it is more likely than

not that evidence of this access will be found in his home, including on digital devices other than the portable device (for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices).

i. Based upon the specific details discovered in the investigation of this case, as outlined below in paragraphs 26 through 33, I believe that Paul Douglas Nida, is a consumer of child pornography residing at the SUBJECT PREMISES, who likely displays characteristics common to consumers of child pornography.

COMPUTER SYSTEMS AND DATA

9. As described above and in Attachment A, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer’s hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).
10. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment A’s definition of “hardware”) can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, accessing the internet, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of

communications and evidence of communications and evidence that reveals or suggests who possessed or used the device.

11. I submit that if a computer or storage medium is found in the place to be searched, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the reasons that follow.
12. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost.
13. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
14. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. This forensic

evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

15. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." An internet browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.
16. As further described in Attachment A, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:
 - a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online

nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage

media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

17. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
18. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
19. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
20. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and

experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

21. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:
 - a. The volume of evidence on storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on site.
 - b. Technical requirements for analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring

expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

22. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment A are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the

contents or ownership appear or are described by people at the scene of the search.

23. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment A. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.
24. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.
25. This warrant authorizes a review of electronic storage media seized, electronically stored information, communications, other records and information seized, copied, or disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and

agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

THE INVESTIGATION

26. On June 3, 2020, I, TFO Damarise Goehring, was acting in an online, undercover capacity (OUC) on Kik Messenger, which is an instant messaging mobile app. I became aware of another Kik user, Doug \$. This specific user's display name was Doug \$, and his user name was doug1610. Hereinafter, this user will be referred to as Doug \$, or as Paul Douglas Nida, who I believe to be one and the same. On this day, June 3, 2020, I was posing as a mother with an infant daughter. Doug \$ added me to a Kik Group entitled "No Limits (verify with Admin)". Since being added to the group, Doug \$ has distributed 6 "Mega.NZ" links to me. The Mega.NZ links distributed by Doug \$ gave me access via a digital link to numerous images of child pornography. I am aware that Mega.NZ is a hosting entity located in New Zealand. I shared these links with SA Moore, with the Federal Bureau of Investigation, who clicked on or activated on the links sent by Doug \$ and, when he did, numerous images of child pornography appeared which were contained within the link. Doug \$ also distributed to me photographs of what he claims are of his 16-year-old daughter and his nieces depicted on a boat. At least one of the photographs depicts an image of one of the young girls in a bikini, and the photograph is zoomed in to her crotch area. Doug \$ informed me that he resides in the Chattanooga, Tennessee area and was 54 years

old. Additionally, he stated in private chats that he has two sons age 30 and 33, and one daughter age 16. Doug \$ wrote that his oldest son lives in Tennessee, the other resides in Florida, and his daughter resides in Knoxville, Tennessee. He also wrote that his favorite content is "Mother Daughter." On June 5, 2020, Doug \$ distributed a Mega Link to me that was 3.16GB in size and was entitled "videos." I shared this link with SA Moore who opened it with the Mega app and the link contained numerous videos and images of child pornography as defined in 18 U.S.C. 2256(8), as well as bestiality videos. These videos were located under sub file folders entitled:

- Animals, Daughter dads
- Girls under 6 sex
- Kids together
- Mom kids
- Young girls alone
- Young with animal

Agent Moore viewed a number of the videos distributed to me via the Mega Link and he observed the following depictions:

Videos of vaginal sex between girls under the age of 12 and adult males.

- Videos of girls under the age of 12 performing oral sex on adult men and adult men and adult women performing oral sex on girls under the age of 14.
- Videos of girls under the age of 16 engaged in sexually explicit conduct with animals.
- Videos of adult men digitally penetrating the vaginas of girls under the age of 12.

- Videos of adult men inserting sex toys into the vaginas of girls under the age of 12.
27. Notably, Doug \$ has expressed a sexual interest in my notional infant-aged "daughter" and has shown an interest in meeting for sexual activity with me and the infant. He has also distributed multiple infant-aged images of child pornography to me.
 28. Recently, on August 12, 2020, Doug \$ sent me a child pornography video of an adult male attempting to digitally penetrate a female toddler and then ejaculating on her vagina and stomach.
 29. Administrative subpoenas were issued to Kik and, on July 15, 2020, SA Moore received a Kik/Media Labs return for Doug \$ which revealed that the user utilizing Doug \$, registered for Kik using an Android device and solely utilized AT&T Cellular data to access Kik. This user registered for Kik with the following email address: dournida@yahoo.com.
 30. SA Moore then performed a CLEAR search. CLEAR is a search platform used by law enforcement, that I have used on other occasions and have found it to be reliable. A CLEAR search for DOUG NIDA in Chattanooga, Tennessee, revealed the following identifying information:

PAUL DOUGLAS NIDA

SSN: 257-31-1000

DOB: 06/14/1963

ADDRESS: 3693 SHIRL JO LN #C Chattanooga, TN 37412

TN DL: 071193985

The utility service address in CLEAR was 3657 Shirl Jo LN # C Chattanooga, TN 37412

Google maps refers to the address as both 3695 Shirl Jo Lane and 3657 Shirl Jo Lane.

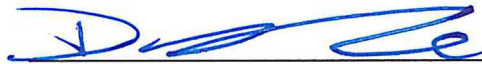
31. Noting that the CLEAR search, the utility service address, and Google maps refer to the same location using different numbers, I conducted research into the differing address numbers. Research into the differing numbers revealed 3693 Shirl Jo LN Apartment C number no longer exists, and that Google's reference to both 3695 and 3657 refer to the same exact location. Research showed that there is no 3695 that exists independently from 3657. Research showed that at some point the address was changed to 3657 Shirl Jo LN Apartment C. I believe based on further investigation that these addresses are one and the same and that Paul Douglas Nida currently resides at this 3657 Shirl Jo LN. As described below, S.A. Moore has conducted surveillance at 3657 Shirl Jo LN and has observed Paul Douglas Nida walk out of 3657 to wheel his trash can to the road. S.A. Moore will accompany me during the execution of the search warrant and will direct law enforcement officials to 3657, which is where he observed Nida exit. Hereinafter, I will refer to this address collectively as 3657 Shirl Jo LN. Technically, this address is within the city limits of East Ridge, Tennessee, which is a small community that abuts Chattanooga and which is a suburb city of Chattanooga.
32. I performed an NCIC search for PAUL DOUGLAS NIDA, which revealed a driver's license photograph that matched the photographs that Doug \$ sent to me

of himself. The address on the driver's license states that Paul Douglas Nida lives at 3695 Shirl Jo LN, Apartment C. A car title search revealed that Nida's car title shows his address as 3657 Shirl Jo LN, Apartment C. Again, I believe that these addresses are one and the same and research shows that these addresses do not exist independent of one another. A Twitter page, @doug_nida, revealed additional photographs matching the individual Doug \$ supplied me wherein he posted that he resides in East Ridge, Tennessee.

33. In digital conversations with Doug \$ while Doug \$ was active on Kik, Doug \$ noted that he works and that he was at work at the time. This confirms that Doug \$ was using a mobile device such as a smartphone. Thus, there is probable cause to believe that Nida is using a smartphone to access Kik and to send child pornography. Kik (according to its law enforcement guide) holds itself out to be a "smartphone messenger application." (<https://lawenforcement.kik.com/hc/en-us/articles/360039841472-Law-Enforcement-Guide>).
34. On August 19, 2020, FBI Agent Sam Moore conducted surveillance at 3657 SHIRL JO LN #C, CHATTANOOGA, TN 37412. Prior to conducting surveillance, Agent Moore reviewed both Paul Douglas Nida's driver's license photograph and the image of Nida, which Nida sent to me through Kik. Agent Moore observed Nida in daylight as Nida exited the door to 3657 Shirl Jo LN, #C on August 19, 2020, and watched Nida as he rolled his trash can out to the road. Agent Moore will accompany me in the execution of this search warrant and will direct officers to the exact apartment from which he observed Nida exit.

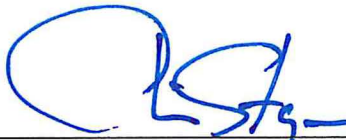
CONCLUSION

35. Based upon information provided in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 2252 and 2252A have been committed and that the items described in Attachment A, attached hereto and incorporated will be found at the residence located at 3657 Shirl Jo LN, #C (Apartment C) and on the person of Paul Douglas Nida, and on Nida's cell phone.



Damarise Goehring, Task Force Officer,
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 20 day of oct, 2020.



HONORABLE CHRISTOPHER H. STEGER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED

1. All visual depictions, including still images, videos, films or other recordings of child pornography or minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, and any mechanism used for the receipt or storage of the same including but not limited to:

Any mobile telephonic device, computer, computer system, and related peripherals including and data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, routers, computer compact discs, CD-ROMS, DVD, thumb drives, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, scanners, digital cameras, webcams, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

2. Any and all documents, records, e-mails, and internet history (in documentary or electronic form) pertaining to the possession, receipt or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256, or pertaining to an interest in child pornography whether transmitted or received.
3. Any and all records, documents, invoices, notes and materials that pertain to accounts with any Internet or Telecommunications Service Providers, as well as any and all records relating to the ownership or use of computer equipment and mobile devices found in the residence.
4. For any computer hardware, computer software, computer-related documentation, or storage media called for by this warrant or that might contain things otherwise called for by this warrant ("the computer equipment"):
 - a. evidence of who used, owned, or controlled the computer equipment;
 - b. evidence of computer software that would allow others to control the items, evidence of the lack of such malicious software, and evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the attachment of other computer hardware or storage media;

- d. evidence of counter forensic programs and associated data that are designed to eliminate data;
 - e. evidence of the times the computer equipment was used;
 - f. passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;
 - g. records and tangible objects pertaining to accounts held with companies providing Internet access or remote storage of either data or storage media; and
 - h. evidence indicating the computer user's state of mind as it relates to the crime under investigation.
- 5. Documents and records regarding the ownership and/or possession of the searched premises.
 - 6. All computer hardware, computer software, computer-related documentation, and storage media.
 - 7. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein.

DEFINITIONS

For the purposes of this warrant:

- A. "Computer equipment" means any computer hardware, computer software, computer-related documentation, storage media, and data.
- B. "Computer hardware" means any electronic device capable of data processing (such as a computer, smartphone, cellular telephone, or wireless communication device); any peripheral input/output device (such as a keyboard, printer, scanner, monitor, and drive intended for removable storage media); any related communication device (such as a router, wireless card, modem, cable, and any connections), and any security device, (such as electronic data security hardware and physical locks and keys).
- C. "Computer software" means any program, program code, information or data stored in any form (such as an operating system, application, utility, communication and data security software; a log, history or backup file; an encryption code; a user name; or a password), whether stored deliberately, inadvertently, or automatically.
- D. "Computer related documentation" means any material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

E. "Storage media" means any media capable of collecting, storing, retrieving, or transmitting data (such as a hard drive, CD, DVD, or memory card).

F. "Data" means all information stored on storage media of any form in any storage format and for any purpose.

G. "A record" is any communication, representation, information or data. A "record" may be comprised of letters, numbers, pictures, sounds or symbols.

ATTACHMENT B

DESCRIPTION OF LOCATION TO BE SEARCHED

The person of Paul Douglas Nida. The residence at 3657 Shirl Jo LN Apartment C, East Ridge, Tennessee, TN 37412, which is located as follows: As you turn onto Shirl Jo Ln from John Ross Rd, it is the first building on the right. Apartment C is the apartment closest to John Ross Rd. The building is gray in color at the top and then white painted brick at the bottom. Mr. Nida's apartment has the letter "C" on the front door.

B1 depicts Paul Douglas Nida in an image provided to me from Doug \$ via Kik.

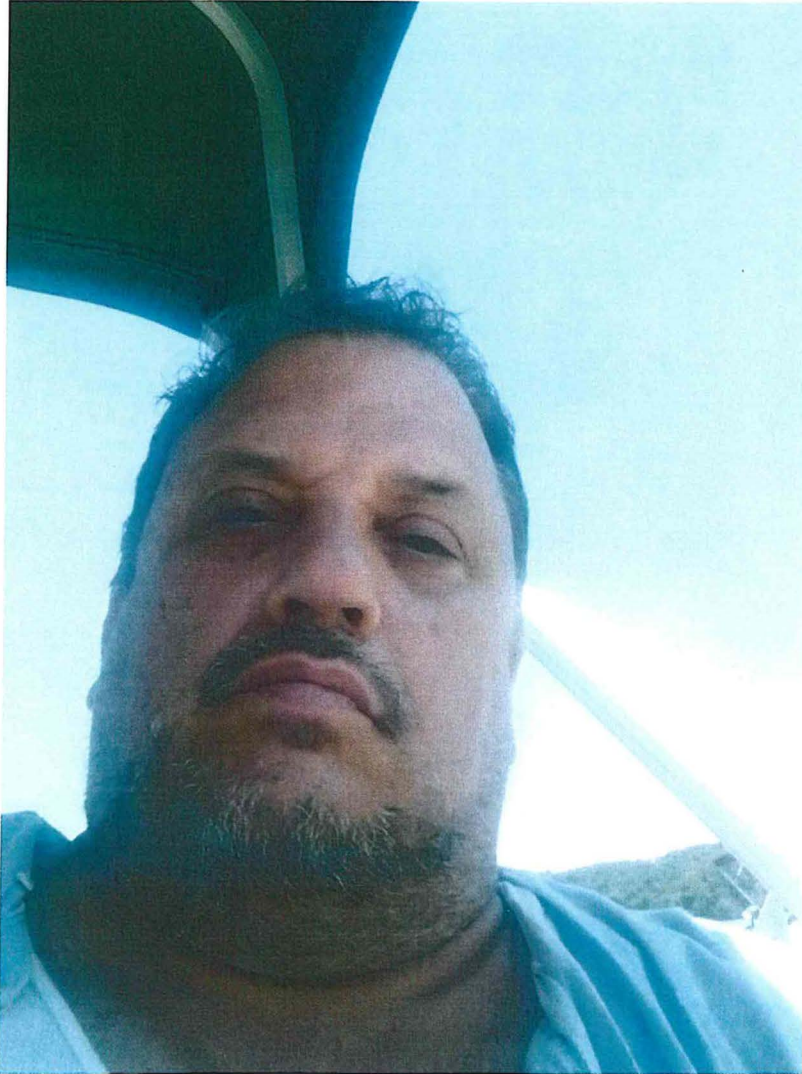
B2 depicts Paul Douglas Nida pictured during surveillance on August 19, 2020.

B3 is Paul Douglas Nida's driver's license photograph.

B4 is an image of 3657 Shirl Jo LN Apartment C, East Ridge, Tennessee, TN 37412 taken during surveillance by Agent Moore on August 19, 2020, which shows the current color of the building and a yellow arrow was added to give the precise location of Apartment C.

B5 is a close up image of 3657 Shirl Jo LN Apartment C, East Ridge, Tennessee, TN 37412 taken during surveillance by Agent Moore on August 19, 2020, which shows the letter C on the door.

B1



B2



B3



B4



B5



